IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF ARKANSAS
FAYETTEVILLE DIVISION

UNITED STATES OF AMERICA	)	
	)	
	)	
v.	)	**No. 5:15CR50087-001**
	)	
	)	
ANTHONY JEAN	)	

SUPPLEMENT TO DEFENDANT'S MOTION TO COMPEL

Comes now the defendant, Anthony Jean, by and through undersigned counsel, and respectfully submits this supplement to Defendant's motion to compel, Doc. 28, and for his motion states:

1. Mr. Jean filed a motion to compel evidence on June 10, 2016, Doc. 19. A hearing on Defendant's motion was held on October 11, 2016. At that hearing, the Court heard testimony regarding the materiality of evidence requested as it pertains to Mr. Jean's case. The Court stated that should it find that the evidence requested is material such that it would justify forcing the Government to reveal it, it would then contact the parties to address the framework addressing the law enforcement privilege.

2. On October 19, 2016, this Court entered an order requesting the Government prepare a confidential brief for in camera review addressing the subject of the qualified law enforcement privilege. Via email on October 20, 2016, this Court notified counsel that it would accept additional briefing on any legal arguments addressing the law enforcement privilege.

3. Defense counsel incorporates by reference all the arguments in Defendant's motion to compel, Doc. 28.

4. It addressing the law enforcement privilege, the Government cites the cases *United States v. Roviaro*, 353 U.S. 53 (1957), *United States v. Van Horn*, 789 F.2d 1492 (11th Cir. 1986), and *United States v. Rigmaiden*, 844 F. Supp. 2d 982 (D. AZ, 2012), for the position that disclosure of the evidence would hinder investigations, and that the evidence requested is not material. Doc. 30 at pgs. 8-13. It is important to note that in each of those cases, the sensitive information/tools utilized by law enforcement never left the government's control. In *Roviaro*, the Government's informer was in a car with the defendant and a concealed officer, and was under surveillance by other officers. *Roviaro*, 353 U.S. at 56. In *Van Horn*, officers installed a microphone in the suspect's office, and the government knew where the device was at all times and retrieved it after the investigation. In *Rigmaiden*, officers used a cellular site simulator to locate a wireless aircard that assisted in identifying the defendant.

In contrast to Mr. Jean's case, part of the evidence requested in this case, the exploit, was not under the Government's exclusive control. It was transmitted to thousands of unknown computers, located around the world. In order to hack these computers and execute the software, the Government had to first transmit a copy of the exploit to each computer. The Government could hardly be said to have taken care to maintain exclusive control of the requested evidence. Moreover, the Government assumed the risk that someone might save a copy of the exploit, and subsequently publish it.[1] Thus, once the Government sent copies of its exploit over the internet to thousands of people, it effectively waived any argument of sensitive information pursuant to the law enforcement privilege.

[1] This very thing happened in 2013, in previous operation, when the Government delivered a NIT to visitors to "TorMail." One or more users caught the act, saved and published a copy of the exploit, and then alerted the public. See, https://www.wired.com/2013/09/freedom-hosting-fbi/

5. Addressing the Government's reasons for invoking the of law enforcement privilege, it argues that disclosure of the requested evidence would be harmful to the public interest, could diminish the future value of important investigative techniques, allow individuals to devise measures to counteract these techniques to avoid detection, discourage cooperation from third parties, and other harmful consequences. Doc. 30 at pg. 8. The Government argues that the defense, who has not had the opportunity to analyze the evidence, presented no evidence to suggest the evidence acted in a way inconsistent as suggested by the Government, and that the defense requests were speculative and conclusory. Doc. 30 at pg. 13.

6. First it is important to note that the Government's position does not explain how a protective order, which the defense has agreed to, would not be sufficient to protect the information. Secondly, the Government is using its non-disclosure of the evidence as both a shield in the form of the privilege, and a sword by alleging that the defense has failed to provide sufficient information that the evidence requested is material, without the defense having the opportunity to examine the evidence. This places the defense in a significant disadvantage at trial.

In regards to the Government's arguments that defense's position involves speculation, there have been at least some instances involving hacking techniques as argued by defense. A Seattle police raided the home of two people who use the Tor network, based on an allegation that their IP addresses had been linked to child pornography, when in fact illicit traffic had merely passed through their connection to the network. Martin Kaste, "When a Dark Web Volunteer Gets Raided by the Police," NPR.org (April 4, 2016).[2] Similarly, a few years ago independent experts determined that an NIT-type malware used by German law enforcement had left target computers vulnerable to "Trojan" viruses. These viruses, among other problems, allowed third parties to

[2] Available at: http://www.npr.org/sections/alltechconsidered/2016/04/04/472992023/when-a-dark-web-volunteer-gets-raided-by-the-police

remotely control the computer. See "Chaos Computer Club Analyzes Government Malware," available at: https://ccc.de/en/updates/2011/staatstrojaner ("We were surprised and shocked by the lack of even elementary security in the [police] code. Any attacker could assume control of a computer infiltrated by the German law enforcement authorities."). *See also* CBS News, "Viruses Frame PC Owners for Child Porn," November 9, 2009 ("Of all the sinister things that Internet viruses can do, this might be the worst: They can make you an unsuspecting collector of child pornography.").[3]

7. The FBI has a recent documented history of concealing key information from defendants and courts. In *State v. Andrews*, 227 Md. App. 350, 374-77 (Md. Spec. App. 2016), the court affirmed a suppression order in part because it found that local police and prosecutors had been instructed by the FBI not to disclose, even if ordered to do so by a court, the capabilities of the FBI's "Stingray" cell phone surveillance technology. After initially hiding its use of "Stingray" entirely in warrant applications and discovery, agents and officers went on to mislead the courts about the fact that it captures more than just basic location information, as the FBI had claimed. As the court noted, the FBI's obstruction of disclosure "from special order and/or warrant application through appellate review – prevents the court from exercising its fundamental duties under the constitution." *Id*. at 375. "It is self-evident that the court must understand why and how [a] search was conducted," and "[t]he analytical framework requires analysis of the functionality of the surveillance device and the range of information potentially revealed by its use." *Id*.

As reported on April 20 in USA Today, FBI supervisors have ordered its Engineering Research Facility (ERF) and Technically Trained Agents (which are responsible for developing and deploying NIT's and other "surveillance capabilities") to follow "Special Project

[3] Available at: http://www.cbsnews.com/news/viruses-frame-pc-owners-for-child-porn/

Concealment" protocols for sharing information with Assistant U.S. Attorneys and case agents. Brad Heath, "FBI Warned Agents Not to Share Tech Secrets with Prosecutors," USA Today, April 20, 2016.[4] These protocols require the FBI's technical specialists to withhold information about NIT's and other "techniques" from prosecutors and case agents so that they are unable to share information during discovery or cross-examination. See Exhibit A (two of the internal FBI emails referenced in USA Today).

Given these issues, the central role the evidenced requested played in this case, the law enforcement privilege must give way and the defense should have access to the requested evidence. *See*, *e.g.*, *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012)(access to software used by law enforcement to access computer was crucial to defendant's ability to assess the program and testimony of the FBI agents who used it to build case against him,

WHEREFORE, the defendant, Anthony Jean, respectfully submits this as a supplement to his motion to compel, Doc. 28, and for all other relief to which he may be entitled.

Respectfully submitted,

BRUCE D. EDDY
FEDERAL PUBLIC DEFENDER
WESTERN DISTRICT OF ARKANSAS

By: /s/ Joe Alfaro
Joe Alfaro
Assistant Federal Public Defender
3739 N. Steele Blvd., Suite 280
Fayetteville, AR 72703
(479) 442-2306

[4] Available at: http://www.usatoday.com/story/news/2016/04/20/fbi-memos-surveillance-secrecy/83280968/

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court using the CM/ECF System which will send notification of such filing to the following: Denis Dean, AUSA, and I hereby certify that I delivered a copy to the following non CM/ECF participants: none.

/s/ Joe Alfaro
Joe Alfaro